21. Symmetries

1. Symmetry Groups

We have seen that there are 3 patterns of trees on 5 vertices and yet there are 125 trees.

Here we have a collection of operations that take trees into other trees that look just like them. Such operations are called symmetries.

Here the symmetries are all the permutations of the five labels on the vertices. A tree looks like another to us, if we can get it from the other by switching labels.

A permutation of a set is a reordering of its elements.

Permutations can be described in two ways:

One is by listing the new ordering that replaces 1, . . . ,n. Thus 1 3 5 4 2 represents the permutation that takes 1 to itself, 2 to 3, 3 to 5, 4 to itself and 5 to 2.

Another way to represent a permutation is **to put all the cycles of the permutation inside parentheses**. This same permutation is then described as (1) (2,3,5) (4).

There are n! permutations of n symbols. Still another way to describe them is by an n by n matrix whose entries are either 0 or 1. There is exactly one 1 in each column and row; the 1 entry in the j-th column is the element that j is taken to in the permutation.

Thus the example above corresponds to the matrix

1	0	0	0	0
0	0	0	0	1
0	1	0	0	0
0	0	0	1	0
0	0	1	0	0

In general, symmetries of any system form a mathematical structure called a group.

A group is a set of entities that has a "law of composition" which allows you to assign a single element to each pair of elements. The set must include an identity element, and each element must have an inverse which when composed with it produces the identity element. **Finally, the composition law must be associative**, so that if you compose A and
B and the result with C you get the same answer as if you compose A with the result of composing B and C.

Symmetry operations are groups with the law of composition that reads: **A composed with B, written as AB, means: perform operation B; then perform A**. (We do things backwards to make what would ordinarily be clear into something inscrutable. If you do not like that please stand on your head. Then our notation will make perfect sense.)

The identity is the operation which does absolutely nothing. We never defined what a symmetry operation could be, but there are two properties that are essential.

One is: **A symmetry operation followed by another is a symmetry operation**, which means that if A is a symmetry
and B is then B followed by A is one also. This implies that performing two permutations does define a law of composition and produces an element of the set of symmetries for every pair of elements composed..

The other is reflexivity: a symmetry must be reversible. **If doing something maintains symmetry, then undoing it does as well**. This means that each symmetry has an inverse which is also a symmetry.

Associativity
of the law of composition of symmetries is merely the statement that doing A and then B and then C is the same as doing A and then B and then C. It is a direct consequence of the nature of the order of time.

You are used to groups because integers and rational numbers and real numbers and complex numbers and numbers mod n for any n form groups under the law of composition called addition. Also rational real and complex numbers and numbers mod p for any prime p, form groups under multiplication when 0 is omitted (and numbers relatively prime to n mod n form one s well.)

Because of this fact
we often describe the law of composition of a group as multiplication or addition, which are shorter to write or say than "law of composition". Thus we call AB the product of A and B or sometimes the sum of A and B, when they mean, as they do for symmetries, do B then do A.

You should note that groups in general do not have the property that the groups of arithmetic all share: that of commutativity. When you multiply or add numbers, the order in which you do so does not matter. But **when you deal with operations, order does matter.**

My favorite illustration of this fact is the operations of putting on your socks, and of putting your shoes. There is an order of doing these things which works well, and one that does not. If you doubt this try putting on your shoes first.

Any group can be described by what is called its "**multiplication table**". This is a table exactly like the multiplication table of numbers up to 12 that many of us encountered as children at the back of notebooks, except that it includes a row and column for each element of the group and not just the small ones.

Not all multiplication tables define groups. To do so, **each row and column of the table must be a permutation of the group elements,**
(so that the permutation represented in that row or column is invertible) and **the table must obey the associative law.**

When we considered graphs, we noticed that there are graphs and then there are drawings of graphs, which have additional properties, like faces or crossings of edges.

With groups there are **abstract groups**, which are defined by their multiplication table; and
permutation groups which permute objects, and
matrix groups, whose elements are matrices with matrix multiplication as their law of composition.

Every finite group can be considered a permutation group on itself as objects. **Each group element can be considered to act on all the others and to permute them according to its row of the multiplication table**.

Since **any permutation group can be described by matrices**, **every finite group can be written as a group of matrices**. (This means it has a faithful representation by a group of matrices with law of composition given by matrix multiplication.)

However,**a**
given group can be written as a permutation group acting on many other types of objects, and its elements can be described by matrices in many ways.

In fact a group G is said to be **represented by** a group of matrices M if there is a function f that maps the elements of G into those of M that preserves the law of composition; which means that f(A)f(B) = f(AB).

A **representation is said to be faithful, if the function f is invertible**. Not all representations are faithful. In fact the mapping f(A) which takes A into I for all A in G makes the trivial one dimensional matrix group consisting of the single element 1 a representation of every group.

A matrix representation of a group consists of square matrices of some given size, say n by n. **Given two representations, of dimensions m and n, we can compose them by putting the representor of each group element q in the first representation in the upper left m by m corner of an m+n by m+n matrix, and putting q's representor**
in the second representation in the lower right n by n block of the matrix with 0's everywhere else in the matrix.

We can then find a different basis for these matrices which obscures this structure.

A matrix representation is said to be reducible, **if it can be broken up into two representations an m by m one in the upper left corner and an n by n one in the lower right for each of its elements simultaneously after some change of basis.**

If this cannot be done, the representation is said to be irreducible.

Before going on there are two important notions related to groups that we will discuss.

2. Subgroups

First is the notion of a subgroup. H is a subgroup of a group G if H is a subset of G and the composition of any two elements of H lies in H. We sometimes write this statement as **HH=H.**

Given a subgroup H of G, and an element g not in H we can define **the coset gH to be g composed with each element of H.** We can similarly define Hg; one of these is called a left coset and the other a right coset.

When gH and Hg are the same for every g in G we call H a normal subgroup of G.

If H is a normal subgroup of G, then we can define another group, called the factor group G/H, whose

elements are the cosets of H in G. The law of composition of these cosets is aH composed with bH is abH. This works because aHbH is by the definition of normality the same as abHH which is the same as abH since H is a subgroup.

All subgroups of a numerical group are normal, since all elements commute. **These provide many examples of normal subgroups**. Thus if we consider the additive group of integers, there is a subgroup consisting of the even numbers (more generally of the numbers divisible by k for any k.) The factor group corresponding to this group is the group whose elements are the cosets of odd and even numbers, with the 1+1=0 rule. (with
similarly the numbers mod k under addition as the factor group for the subgroup of numbers divisible by k.)

There is a wonderful and simple theorem about subgroups which will be of much use to us, as follows.

If G is any finite group, and H is any subgroup of G, then the number of elements of G is an integer multiple of the number of elements of H. This statement is called Lagrange's Theorem.

We can prove it by showing that **any two cosets, aH and bH have the same number of elements as H itself has, and are either identical or have no element in common.**

That aH and bH
have the same number of elements as H follows from the fact that each consists of that many elements from the a and b rows of the multiplication table of G, which are each permutations of the elements of G so that no repetitions are possible.

If we have ah = bh' for some h and h' in H, then we would have $a = ahh^{-1} = bh'h^{-1}$ so that for any h" in H and we would have $ah"=bh'h^{-1}h"$ which (since HHH=H) means that any member of a's coset is a member of b's and this makes the two cosets identical.

Thus the elements of G can be written in a rectangle one of whose sides is the cardinality of H and the other the number of distinct cosets gH
of H in G. The number of elements of G is therefore the product of the number of elements of G and the number of distinct cosets, when G is finite.

This wonderful fact tells us, for example, that **if the number of elements of G (called G's order) is prime, then its only subgroups are itself and the group consisting of I alone.**

Every element A of every finite group G generates a subgroup which consists of its positive powers: A, A^2, A^3, . . . ,. This sequence must end since G is finite, and the list is obviously closed under multiplication. **The order of this subgroup is also called the order of A**, and by Lagrange's theorem, **the order of G must be an integer multiple of the order of any element.**

A group is said to be cyclic if it is generated by one of its elements. We can deduce here that **any group of prime order is cyclic**,
since the order of any of its elements other than the identity must be the order of the subgroup it generates which can only be the whole group, G.

A group without non-trivial normal subgroups is said to be simple. Not that long ago

mathematicians were able to complete a list of all the simple groups. These include three general classes of matrix groups and a finite number of other weird groups including several of enormous size. And every simple group has a faithful representation as one of these.

Any group of prime order is normal since it has no non-trivial subgroups at all.

Is the group of permutations of n symbols simple?

The answer is no, for n at least 3.

Any permutation can be constructed by starting from the identity permutation and switching pairs of elements. (In its matrix form this corresponds to switching two of the rows of the matrix.) A permutation is called even if it can be constructed by an even number of such switches and odd otherwise. (This corresponds to the determinant of the matrix representation of the permutation being +1 or –1.)

The even permutations of n elements form a subgroup called the alternating group on n elements denoted as A_n. Since this group has only one cofactor other than itself, that cofactor is unique, whether defined from the left or right, and the alternating group is always a normal subgroup.

3. Conjugacy

Two elements of a group, A and B are called conjugates if there is a group element C obeying **AC = CB** which implies $\mathbf{A= CBC^{-1}}$ and $\mathbf{B = C^{-1}AC}$. If A and B are conjugates and B and C are, then A and C are as well.

Exercise: Prove that if A is conjugate to B and C then B is conjugate to C.

We can partition any finite group into blocks called conjugacy classes, such that each pair of members in every block are conjugates of one another.

Among permutation groups, two elements are conjugate if their cycle structure is the same. Thus any two permutations of 7 elements which consist of one cycle of length 3 and another of length 4 are conjugate to one another.

Thus, while there are n! elements of
the group of possible symmetries of n objects (which group is usually denoted as S_n) , there are only a number of conjugacy classes given by the number of partitions of n into blocks.

And how many of these are there? How many partitions of n into blocks are there which is how many conjugacy classes S_n the symmetric group on n elements possesses?

Let us look at what happens when n is small; suppose for example n=9.

We will describe our partitions by omitting fixed points, correspond to blocks of size 1. This means that the difference between n and the sum of the block sizes shown is made up of blocks of size 1.

Then we have the partition that is all 1's, then (2), (3). (4), (2,2), (5), (3,2), (6), (4,2) , (3,3), (2,2,2), (7), (5,2), (4,3), (3,2,2), (8), (6,2), (5,3), (4,4), (4,2,2), (3,3,2), (2,2,2,2), (9), (7,2), (6,3), (5,4), (5,2,2), (4,3,2), (3,3,3), (3,2,2,2) . There are a total of thirty of them. On the other hand there are 9! or 362880 elements of the symmetric group on 9 symbols.

We can count these numbers on a spreadsheet by use of the following properties.
Let the number of partitions of n into k blocks be p(n,k).

Then we have

$$p(0,0) = 1,$$

$$p(n,k)=0 \text{ for } k>n \text{ or } k<0,$$

and

$$p(n,k)= p(n-1,k-1) +p(n-k,k)$$

The last of these statements represents the fact that the partitions that include a block of 1 are, if we ignore that block, partitions of n-1 into k-1 blocks; while partitions which have all blocks at least 2 become partitions of n-k into k blocks if we subtract 1 from each block.

We can express the condition that a subgroup is normal by the statement that its elements consist of complete conjugacy classes.

We consider some examples. Consider the alternating groups on 3, 4, 5, and 6 objects.

The elements of these groups are the even permutations of the objects, which are those with are those with an even number of even cycles. They are

For n= 3: (1,1,1) there is one such element, the identity,
and (3) there are two three cycles of three elements (123) and (132).
And this group has three elements.

In this case the alternating group is a cycle and has no normal subgroups.

For n=4: (1,1,1,1) the identity again
(2,2) there are three of these. (12)(34), (13)(24), and (14)(23)
(3,1) there are 8 of these, namely (1)(234), (1)(243), (2)(134), (2)(143), etc.

The alternating group has 12 elements. The first two conjugacy classes here have four elements, and form a subgroup. This is a normal subgroup of S_4.

For n=5: (1,1,1,1,1) the identity again
(3,1,1)
20 of these; two ways of cycling three elements and C(5,2) ways of picking out two not to cycle
(2,2,1) 15 of these, 5 objects to leave out and 3 ways to split 4 in two.
(5) 24 of these: start with 1 and add the rest in any of 4! orders.

Exercises: 1. Find it above.
2. Write down the multiplication table for the group of permutations of 3 symbols.
3. Find the conjugacy classes for S_6, which is the group of all permutations of six symbols. Prove that its alternating group (denoted by A_6) has no normal subgroups.